Testimony of John S. Leggate C.B.E

Chief Information Officer & Group Vice President
Digital & Communications Technology
BP Plc
United Kingdom

Chairman of the Business Executives for National Security CEO
Roundtable on Digital and Cyber Infrastructure Security

Before the
Committee on Science

U.S. House of Representatives

September 15th, 2005

BUSINESS CONCERNS FOR THE INTERNET

STATEMENT OF THE ISSUE

The Internet is rapidly becoming the backbone of the world economy. This is particularly true for the United States where the use of the Internet underpins many aspects of the US economy and national critical infrastructure (eg energy, water, transportation). Given this fundamental dependency on its continuous availability, the public Internet must be better protected, managed and controlled. In the longer term, the US should take a leadership role in creating the next generation Global Internet.

SUMMARY OF THE ISSUE

The growth of Internet use has been nothing short of extraordinary[1]. Almost by stealth since the dot com collapse, governments, public bodies and large and small scale businesses have been transformed to operate with the Internet as a core piece of business infrastructure. Businesses from all over the world have found the Internet to be a cost effective and reliable business tool. Indeed, in the last few years, in addition to conventional business transactions, many of the controls systems (SCADA) that support national and public utilities are adopting the Internet as a core data transport method[2]. This has resulted in businesses and societies becoming critically dependent on the continuous operation of the Internet[3].

Businesses have moved from dial-up and dedicated point to point leased lines to committing mission critical digital traffic to operate on the Internet, yet with no practical alternative to maintain business continuity. However, the Internet is mostly run by groups of diverse academic and non-profit organizations which operate via loose consensus. Many governments have apparently not yet fully grasped that national and international economies and their citizens are now dependent on this network of networks – i.e. the global communications backbone.

[1] Lazarus Research Group
[2] Internet Security Systems
[3] Jupiter Research

In its current operation the Internet has well known physical and logical security weaknesses both nationally and globally. What is *not* truly known is the potential business impact of these weaknesses on the US and the world economy. Continued operation is presumed, but is in no way guaranteed. This is compounded by the poor understanding of dependency / interdependencies between companies and critical infrastructures supporting nations/ regions

Global competition has driven the need for ever increasing levels of productivity and innovation from businesses and this has driven the demand for cheaper and more ubiquitous communications. The nature of the architecture of the Internet has allowed it to carry an ever increasing variety of services, with ever decreasing costs. These forces are driving applications, services and business processes from every sector onto the Internet. Businesses that fail to exploit these cost and performance advantages are at a competitive disadvantage.

Today, at moment there are some 200 million individuals active on the Internet. . By the end of 2005, at least one billion people will have access to its enormous resources[4]. Also there are as many automated systems - including SCADA systems, CCTV, pipelines, electricity grids, email servers, inventory systems and medical monitoring devices. These systems often communicate over the Internet without human intervention. This machine-to-machine communication is growing dramatically and could supplant interactive use by people in a few years[5].

In 2004, $6.9 trillion of the $55.6 trillion of world wide trade was directly transacted over the Internet[6]. Of the remaining trade there was a significant proportion that relied on supporting activity using the Internet for communication – including specification queries, logistics and links between internal processes within companies. Even financial institutions use the Internet for many routine electronic funds transfers[7]. Significantly, in 2004 and in the US alone, 14.8 million high tech jobs relied directly on the Internet.[8]

In the past there have been attempts to address the issues of security, operational stability and reliability but with limited success. For example, work conducted by the President's Commission on Critical Infrastructure Protection (PCCIP) nearly ten years ago, raised vulnerabilities that are apparently yet to be addressed[9]. It

[4] Meta Research
[5] ZDNet Research
[6] Forrester Research, Inc.
[7] Forrester Research, Inc.
[8] University of Texas-Austin
[9] PCCIP Report 1997

set a goal of a reliable, interconnected, and secure information system infrastructure by the year 2003. Is the context and sense of urgency different today?

This paper explains why the context is now so very different. In the '80s and early '90s companies were not using the Internet in anything like the same way or to the same scale as they do today. Private networks were the common means of communication. The companies providing Internet infrastructure were justified in treating identified weaknesses as rather academic and with little economic importance.

However, things have changed and in ways that often only businesses directly using the Internet can articulate[10]. Companies can, and do, take security measures to protect the systems they run and the services directly under their immediate control. But they can do little, to protect the external network infrastructure on which they rely or even engage in a meaningful dialogue about fundamental performance expectations. Previous work in evaluating risks to the Internet has almost entirely focused around a dialogue between supply-side telecommunications/IT companies and government[11]. We therefore only have half the picture, knowledge of interdependency between supply and demand-side for Internet services clearly needs to be shared.

Even more troubling is that many demand-side organizations do not realise how dependent they are on the Internet. Corporations have become linked to the Internet in ways that are not always easily discerned. For example, a major corporation that depends on a third party's logistical services may be surprised to learn that their supplier communicates internal orders and status using the Internet, or that an electric utility they depend upon has moved its process control network to run over the Internet.

These cascading dependencies all too quickly create 'domino effects' that are not obvious to the corporate customer or to the policymaker. They are usually only discovered during unplanned outages when capabilities begin to degrade or fail in unexpected ways, or are discovered during widely-based crisis management exercises. Businesses and governments can plan for expected failures. But even the best prepared organizations and corporations may be woefully inadequate in responding to complex, low probability, high impact failures. If a large scale Internet outage or significant reduction in performance were to occur, the

[10] See Appendix

[11] National Security Technology Advisory Committee (NSTAC) and the National Infrastructure Assurance Council (NIAC).

unexpected effects on whole sets of industries, utilities and enterprise could have surprisingly large economic and societal impacts.

Whether the failure of the Internet arises through error, a worm-writers experiment, or more directed physical or cyber attacks, vulnerabilities exist and this is a real and present risk. Recent reports about "Cyber attack" attempts being developed and the posting of hacker tools with directions on some of the extremist's websites may be warning signs.

BROADER CONTEXT

It is worth recalling that the Internet was set up as a government sponsored project, with the US government as the primary customer and 'anchor tenant'. Its creation was a bold and dramatic step-out that went on to evolve into a remarkable resource that has significantly exceeded the wildest imaginings of its creators. As a result it is being used far beyond anything envisaged in the original designs.

Since its creation, the Internet has developed rapidly in scale, but its technical design has progressed more through steady incremental evolution than through any step change. The "grass roots" and academically-based standards setting process of the Internet Engineering Taskforce (IETF) has had great success. However, the down-side of this consensus approach is that entity wide coordination and alignment is difficult to achieve and step changes are difficult to implement. Internet standards setters are a community of interest and as such they share interests, but they do not share goals and timescales in the way that a project with a clear mandate does[12].

This diversity of interest has been compounded by the loss of the primary customer, i.e. the US government, driving operational performance requirements, since they have started to use alternative infrastructures for extra critical services. Instead of a single 'anchor tenant', the Internet now has countless customers drawn from many governments, corporations and individual users and is thus driven by a very diverse range of agendas, without a clear priority setting process. This will further slow change and adaptation to the new and emerging context of Internet use.

[12] Drawn from I-space theory. Max Boisot, INSEAD

The question we need to ask is whether incremental change will be sufficient to address the current physical and digital integrity weaknesses. The current deficiencies on the Internet may well be filled by tactical repairs, but the potential gap of predictable demand for high volume traffic with high quality services and the intractable vulnerabilities will require a more radical approach. Arguably the risks we are seeing, illustrated by spreading worms and viruses and underlying common mode weaknesses in technologies and physical infrastructure are systemic and systematic in nature[13]. Systemic and systematic risks can only be addressed through coordinated rather than isolated action. A fact well illustrated by other complex systems such as vaccination statistics and epidemiology in the medical world and in the risk management intervention required in national and global banking systems[14]. Many of these risks have no geographic or country boundaries - impact and influence is global.

The widespread globalization of the Internet also introduces a further development complexity. Scores of countries now have fundamental interests in its evolution and some are even orchestrating local step-changes in technology.[15] However, no country has yet felt able to propose fundamental change on a global basis. Within the US, the Internet is seen in many quarters as the starting point for the National Information Infrastructure (NII). Around the world, there is growing recognition that the set of NIIs (assuming each country commits to developing one) should be compatible with each other in an - as yet - undefined way. Who should take the lead in ensuring this compatibility? There is clearly an important role for government leadership in framing this strategic agenda – with strong collaboration with commerce and business.

In practice, the technical scope of the Internet already goes beyond that defined as "Internet services". Ultimately, the communication pathways must enter the user's machine/other digital devices, pass through layers of software and end up in applications programs. The computer industry, along with the many vendors of computer-related equipment, must play a role in determining how this aspect of the Internet will evolve and therefore form part of the supply-side. A key to the success of the Internet is to ensure that the interested parties have an equitable way of participating in its evolution, including participation in its evolving standards process and technology roadmap. A proper role for

[13] Illustrated by work from the Cooperative Association for Internet Data Analysis (www.caida.org)
[14] Drawn from standard epidemiology texts and banking risk texts and the opinions of banking regulators.
[15] For example, the broad introduction of IPv6 in Korea and Japan

governments would be to oversee this process to make sure that it meets the wide spectrum of public and industry needs.

Yet further complexity and dependency is being introduced by a new breed of service providers who are offering services that will continue to supplant alternative networks. Telephony (through Voice over IP), television, radio and almost all forms of communication are migrating to the Internet or including the Internet as a key component in the communication path.

CONCLUSIONS ON CURRENT POSITION

- There are no clear accountabilities or guarantees for the continuity of operation of the Internet. Even weaknesses known about for some time have not yet been addressed.
- A significant and growing proportion of the world economy is dependent on the Internet.
- The Internet is currently subject to technical and geopolitical risk and therefore not only the US economy, but economies worldwide, are at risk.
- The US Government itself is no longer fully dependent on the Internet, as it has alternative networks at its disposal for critical services. Thus the Internet has moved from having a single 'anchor tenant' to a diverse community of stakeholders without a voice in the operational performance expectations of the current Internet
- New technologies and emergent Internet uses, such as Voice over IP and widespread control system connectivity, are increasing dependency and compounding the risk.

OPTIONS ON THE WAY FORWARD

We would consider a two-pronged approach, to address both the immediate risk and the strategic opportunity:

1. Short Term

To address immediate concerns a series of in-depth and as necessary classified studies, workshops and truly cross-sectoral exercises should be held to allow businesses (that deliver critical aspects of national infrastructure – e.g. energy, transportation and financial) and governments to share critical information

under the **Protected Critical Infrastructure Information (PCII) Program.** The goal of this work would be to map the business reliance upon the Internet against known areas of risk and develop a priority plan to focus actions that are necessary for increasing its robustness and integrity.

The work could start with the scope of the US economy in a global context. Interdependency should then dictate that it be extended in the first instance to other countries from the G8 and EU.

2. Medium Term

There is a need to create the next generation Internet in a form that would be able to handle the emerging demands of business, civil societies and governments. This would include the technical design necessary to meet physical and logical diversity and resilience. In addition, the program should include the development of a Global Internet Management Framework that addresses broad policies and standards, clarity of operational accountabilities, and technology roadmaps. The goal should be to assure the performance and digital integrity of the new Global Internet, in terms of resilience to physical and cyber-security risks, supplier commercial failure, and broader geopolitical risks.

We believe the US should take a leading role in this proposed global initiative.

Thank you for the opportunity to express the views of the business community. I look forward to continuing our conversation as our CEO roundtable at BENS (Business Executives for National Security**)** progresses. We look forward to contributing to the actions that we propose.

APPENDIX – Business Criticality Data

Having recognized the potential for serious negative impact on the US critical national infrastructure in the event of a significant interruption of Internet service, a group of concerned business people carried out an informal survey of key sector companies in early 2005. The graph below shows the findings from that survey, indicating the level of dependency these sectors have on the Internet.